PRIVACY IMPACT ASSESSMENT (PIA)

For the

Talent Action Communicator (TAC)
Department of the Navy - NAVSEA - PEO IWS

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: DITPR ID: 8006 DITPR-DON ID: 21449
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI UII: 007-000002325

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier N07510-1, N05230-1, T7335

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number TAC does not collect PII from members of the public.

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

SORN N07510-1, Naval Audit Service Information Management System (NASIMS) (April 05, 2011, 76 FR 18738), authorities:

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 5013, Department of the Navy; 10 U S.C. 5014, Office of the Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; 5 U.S.C. 301, Departmental Regulations; DoD Directive 8320.1, DoD Data Administration; DoD Manual 7600.7-M, DoD Audit Manual; SECNAVINST 7510.7F, Department of the Navy Internal Audit and E.O. 9397 (SSN), as amended.

SORN N05230-1, Total Workforce Management Services (TWMS) (October 20, 2010, 75 FR 64715), authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; CNICINST 5230.1, Total Workforce Management Services; OPNAVINST 3440.17, Navy Installation Emergency Management Program and E.O. 9397 (SSN), as amended.

SORN T7335, Defense Civilian Pay System (DCPS) (March 13, 2014, 79 FR 14241), authorities:

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. Chapter 53, 55, and 81; and E.O. 9397 (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Talent Action Communicator (TAC) is an architecture that provides web-enabled applications to meet operational requirements for daily business processing needs and to enhance and complement the use of Standard Systems including Defense Civilian Personnel Data System (DCPDS), Defense Civilian Payroll System(DCPS), and Total Workforce Management System (TWMS). These applications provide automation of business processes to collect business information not currently collected by those Standard Systems.

TAC applications include the Electronic Telework Agreement Tool (eTAT), Electronic Position Requirement Document (ePRD) tool, Hiring Tracker, Onboarding Tracker, and others. These tools are used by various NAVSEA HQ and Enterprise organizations.

PII collected: Name, Security Clearance, Financial Information: employee salary data, pay plan, series or rank/rate, home address, home email, home and cell phone #, Education information: degrees obtained, years graduated, concentration/major and certifications earned, Employment information: employee salary data, pay plan, series or rank/rate, and DoD ID number.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

There are several risks associated with the PII collected pertaining to compromise of US Navy civilian, military, and contractor personnel and financial information. Unauthorized access of this information could expose this information to individuals without proper authority to view or if compromised to the world at large; compromising reputations or causing embarrassment. To protect against this, all electronic PII is closely protected through role and rule based access control. This ensures that only the proper people have access to view the PII, only the PII that they need, not all of it, once entered into the system. All access is determined by two factor authentication using the CAC and then additional rules/roles are granted to the appropriate users.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. NAVSEA HQ and Enterprise organizations

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

PII that is collected from the individual using electronic forms may choose not to enter information in to the form. Other PII that originates from systems of record have no means of objection because they are not collected directly from the user.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

PII that is collected from the individual using electronic forms provide consent by using the form and by reading and agreeing to the Privacy statement associated with the application. Other PII that originates from systems of record have no means of consent because they are not collected directly from the user.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [ ] **Other**
- [ ] **None**

Describe each applicable format.

Contained on the electronic form that collects information directly from the individual.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.